Kỷ yếu Hội nghị Khoa học Quốc gia lần thứ IX "Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR'9)"; Cần Thơ, ngày 4-5/8/2016
DOI: 10.15625/vap.2016.00021

GIẢI PHÁP PHÁT HIỆN TẤN CÔNG NGẬP LỤT TRÊN MẠNG MANET

Lương Thái Ngọc[1], Võ Thanh Tú[2]

[1] Khoa Sư phạm Toán – Tin, Trường Đại học Đồng Tháp
[2] Khoa Công nghệ Thông tin, Trường Đại học Khoa học, Đại học Huế

ltngoc@dthu.edu.vn, vttu@hueuni.edu.vn

***TÓM TẮT**—Tấn công ngập lụt cản trở quá trình khám phá tuyến và tăng hao phí truyền thông của giao thức định tuyến AODV trên mạng MANET. Trong bài báo này, chúng tôi đề xuất giải pháp xây dựng tác tử di động bảo mật SMA có khả năng phát hiện tấn công ngập lụt, đồng thời tích hợp SMA vào thuật toán khám phá tuyến của giao thức AODV tạo ra giao thức an ninh tên là SMA-AODV. Sử dụng NS2, chúng tôi đánh giá tác hại của tấn công ngập lụt đến giao thức AODV và hiệu quả phát hiện tấn công của giao thức an ninh SMA-AODV trong môi trường mạng có các nút di chuyển ngẫu nhiên.*

***Từ khóa**—AODV, SMA-AODV, MANET, giao thức, tấn công ngập lụt.*

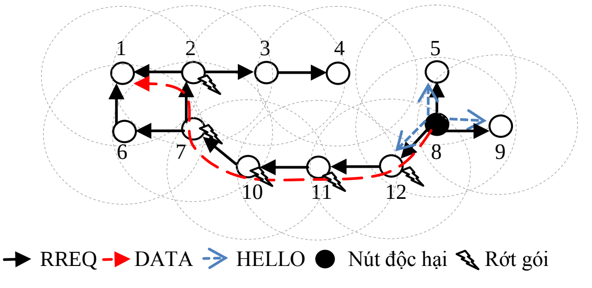
I. GIỚI THIỆU

Mạng tùy biến di động (MANET) là một mạng không dây đặc biệt, với ưu điểm là khả năng hoạt động độc lập không phụ thuộc vào cơ sở hạ tầng mạng cố định, chi phí thấp, triển khai nhanh và tính di động cao. Các nút trong mạng MANET phối hợp với nhau để truyền thông nên đảm nhận chức năng của bộ định tuyến. [1]

Dịch vụ định tuyến được cung cấp tại tầng mạng (Network Layer) là mục tiêu của nhiều loại tấn công từ chối dịch vụ (DoS [3]), tiêu biểu là tấn công ngập lụt (flooding attacks [4]). Hình thức tấn công này được thực hiện bằng cách nút độc hại gửi tràn ngập các gói hệ thống cho các nút không tồn tại trong mạng, hoặc truyền một lượng lớn các gói dữ liệu vô ích để gây nghẽn mạng. Kết quả là tạo ra bão quảng bá gói tin trên mạng, làm tăng hao phí truyền thông, giảm khả năng đáp ứng tại mỗi nút vì phải xử lý các gói tin không cần thiết. Hình thức tấn công này dễ dàng thực hiện với các giao thức định tuyến theo yêu cầu, tiêu biểu như giao thức AODV. Giao thức AODV [5] sử dụng cơ chế khám phá tuyến khi cần thiết rất phù hợp với mạng MANET. Nút nguồn muốn giao tiếp với nút đích mà không có tuyến đường đến đích thì nguồn phải khởi động quá trình khám phá tuyến bằng cách quảng bá gói yêu cầu RREQ. Nút đích trả lời tuyến về nguồn bằng cách gửi gói trả lời RREP, gói HELLO và RERR được sử dụng để duy trì tuyến. AODV là giao thức tiêu biểu thuộc nhóm giao thức định tuyến theo yêu cầu nên tin tặc dễ dàng thực hiện tấn công ngập lụt trên giao thức này, tiêu biểu là tấn công ngập lụt gói HELLO, gói RREQ và gói DATA [6][7].

a) Ngập lụt gói HELLO

Gói HELLO được phát định kỳ để thông báo sự tồn tại của nút với láng giềng trong mạng không dây, đây là điểm yếu bị tin tặc lợi dụng để phát tràn ngập gói HELLO buộc tất cả các nút láng giềng phải tiêu tốn tài nguyên và thời gian xử lý gói tin không cần thiết. Hình thức tấn công này chỉ gây hại đến các nút láng giềng của nút độc hại.



Hình 1. Mô tả tấn công ngập lụt trên mạng MANET

b) Ngập lụt gói DATA

Hình thức tấn công này chỉ gây hại tại một số nút trong mạng, để thực hiện tấn công, nút độc hại phát quá mức gói DATA đến một nút bất kỳ trên mạng, điều này ảnh hưởng đến khả năng xử lý của các nút tham gia định tuyến dữ liệu, tăng hao phí băng thông không cần thiết, gây nghẽn mạng và rớt gói.

c) Ngập lụt gói RREQ

Gói yêu cầu tuyến RREQ được sử dụng để thực hiện khám phá tuyến khi cần thiết, vì thế tin tặc lợi dụng gói này để phát quảng bá quá mức làm tràn ngập lưu lượng không cần thiết trên mạng. Tấn công ngập lụt gói RREQ là gây hại nặng nhất, bởi nó ảnh hưởng đến khả năng khám phá tuyến của tất cả các nút khác trong hệ thống, tạo ra các cơn bão quảng bá gói tin trên mạng để chiếm dụng băng thông, tiêu hao tài nguyên tại các nút và tăng hao phí truyền thông.

Tiếp theo, bài báo trình bày các công trình nghiên cứu liên quan đến phát hiện, ngăn ngừa tấn công. Phần 3 trình bày giải pháp xây dựng tác tử di động bảo mật (SMA) và tích hợp SMA vào cơ chế khám phá tuyến của AODV nhằm phát hiện tấn công ngập lụt. Phần 4 trình bày kết quả đánh giá bằng mô phỏng trên NS2 và cuối cùng là kết luận.

II. CÔNG TRÌNH NGHIÊN CỨU LIÊN QUAN

Thời gian qua, đã có một số nghiên cứu phòng ngừa tấn công ngập lụt, các giải pháp đã đề xuất chủ yếu tập trung theo hướng *ngăn ngừa* và *phát hiện* tấn công.

Các giải pháp ngăn ngừa tấn công sử dụng cơ chế "chứng thực, toàn vẹn và chống chối từ" dựa trên nền tảng chữ ký số hoặc hàm băm có ưu điểm là khả năng bảo mật rất cao, có thể ngăn ngừa nhiều hình thức tấn công xuất hiện, tiêu biểu như: SAODV [8], ARAN [9], SEAR [10], và SEAODV [11]. Tuy nhiên, thời gian khám phá tuyến lớn là một trở ngại khi ứng dụng vào thực tế. SAODV [8] được tác giả Zapata cải tiến từ AODV có thể ngăn ngừa tấn công mạo danh. Tuy nhiên, tồn tại của SAODV chỉ hỗ trợ chứng thực từ đầu-cuối (end-to-end), không hỗ trợ chứng thực tại mỗi nút (hop-by-hop) nên nút trung gian không thể chứng thực gói tin từ nút tiền nhiệm. Ngoài ra, SAODV chưa có cơ chế quản lý cấp phát khóa cho nút, nút độc hại có thể vượt qua rào cản an ninh bằng cách sử dụng bộ khóa giả mạo. Sanzgiri đã đề xuất giao thức ARAN [9] tiến bộ hơn SAODV, gói khám phá tuyến RDP trong ARAN được ký và chứng thực tại tất cả các nút trung gian (hop-by-hop) và chứng thực end-to-end. Ngoài ra, ARAN đã bổ sung cơ chế quản lý cấp phát khóa cho nút. SEAR [10] được Li thiết kế sử dụng hàm băm để xây dựng bộ giá trị băm gắn với mỗi nút, được dùng để chứng thực các gói tin khám phá tuyến. Trong SEAR, định danh (ID) của nút được mã hóa cùng với giá trị SN và HC nên ngăn ngừa tấn công lặp tuyến. Tương tự, SEAODV [11] được phát triển từ AODV bằng cách sử dụng lược đồ chứng thực HEAP với khóa đối xứng và hàm băm để bảo vệ gói tin khám phá tuyến. Thông qua mô phỏng, tác giả đã cho thấy SEAODV bảo mật hơn và có hao phí truyền thông thấp hơn AODV.

Ngược lại, các giải pháp phát hiện tấn công có ưu điểm là ít ảnh hưởng đến chi phí khám phá tuyến, tuy nhiên khả năng an ninh không tốt bằng các giải pháp theo hướng ngăn ngừa tấn công. Trong [4], Ping đã trình bày một giải pháp an ninh chống lại tấn công ngập lụt dựa trên tiến trình xử lý gói RREQ gọi là phương pháp FIFO. Tác giả cho rằng độ ưu tiên của một nút tỉ lệ nghịch với tần số phát sóng RREQ. Các nút thực hiện yêu cầu tuyến quá nhiều sẽ có ưu tiên thấp và sẽ bị loại khỏi quá trình định tuyến. Tuy nhiên, chi tiết chọn giá trị ngưỡng ưu tiên để phát hiện tấn công ngập lụt gói RREQ chưa được trình bày cụ thể. Vấn đề này được khắc phục trong [12], tác giả Ping cũng đã trình bày giải pháp phát hiện tấn công ngập lụt gói RREQ, gói DATA. Để có thể phát hiện tấn công ngập lụt gói RREQ, một giá trị ngưỡng được thiết lập dựa vào dữ liệu của tất cả láng giềng. Ngoài ra, vấn đề phát hiện tấn công ngập lụt gói DATA cũng được trình bày dựa vào dữ liệu nhận được tại tầng ứng dụng. Trong [7], Jiang đề xuất một hệ thống tường vệ kép (DDWS) dựa trên kỹ thuật tiết kiệm năng lượng nhằm giảm thiểu tác động của các cuộc tấn công ngập lụt trong giao thức định tuyến AODV. Dựa trên thông số RREQ RATE-LIMIT định nghĩa trong tiêu chuẩn RFC, một nút mạng khởi tạo RREQ được ưu tiên theo tốc độ dòng chảy với ba cấp độ: hợp pháp, vừa phải và mạnh mẽ. Các gói RREQ nhận được từ một nút có một ưu tiên hàng đầu được chuyển tiếp, ngược lại sẽ bị loại bỏ. Đối với các nút có một ưu tiên vừa, chính sách nâng cấp và hạ cấp độ ưu tiên được áp dụng theo sự thay đổi tốc độ dòng chảy RREQ của nút. Trong [13], Desilva đã trình bày về tấn công ngập lụt gói RREQ và tác hại đến thông lượng mạng dựa trên số lượng các nút độc hại. Để giảm thiểu những ảnh hưởng của các cuộc tấn công ngập lụt, họ đề xuất một lược đồ thống kê gói tin hủy thích ứng. Phương pháp này dựa trên kỹ thuật đánh giá độ trễ ngẫu nhiên để theo dõi các gói tin vừa nhận được trong một khoảng thời gian. Cuối cùng, hồ sơ của một nút được tạo ra và giá trị ngưỡng được tính vào cuối mỗi kỳ lấy mẫu. Giá trị ngưỡng này được sử dụng để nhận biết xuất hiện tấn công ngập lụt gói RREQ hoặc bình thường. Tương tự, trong [14] tác giả Balakrishnan đã trình bày giải pháp thêm thành phần mới vào mỗi nút có nhiệm vụ theo dõi ngưỡng giới hạn số gói tin yêu cầu tuyến của tất cả láng giềng. Giải pháp này đã giải quyết vấn đề phát hiện tấn công ngập lụt gói RREQ, nhưng chưa giải quyết vấn đề tấn công ngập lụt gói DATA.

III. GIẢI PHÁP PHÁT HIỆN TẤN CÔNG NGẬP LỤT

Trong ba hình thức tấn công ngập lụt trên giao thức AODV gồm tấn công ngập lụt gói HELLO, RREQ và DATA thì tấn công ngập lụt gói RREQ là nguy hại nhất vì nó dễ dàng tạo ra bão quảng bá. Bài báo này tập trung vào giải pháp phát hiện hình thức tấn công ngập lụt gói RREQ bằng cách đề xuất tác tử di động bảo mật mới tên là SMA.

1. Đề xuất tác tử an ninh SMA (Security Mobile Agent)

Tác tử [15] là một thực thể vật lý hoặc mô hình logic có tính tự trị, tính di động, tính thông minh, tính thích nghi, tính cộng tác và tính an ninh là điểm quan trọng của SMA. Khi xây dựng mô hình kiểm tra an ninh trong MSA nhằm phát hiện tấn công ngập lụt gói RREQ, chúng tôi sử dụng một số khái niệm liên quan như: Thời gian khám phá tuyến, khe thời gian khám phá tuyến và khe thời gian khám phá tuyến tối thiểu.

- *Thời gian khám phá tuyến* là khoảng thời gian từ lúc thực hiện khám phá tuyến đến khi nhận trả lời tuyến được tính theo công thức 1, trong đó s là thời điểm khám phá tuyến, e là thời điểm nhận trả lời tuyến.

$$t = e - s \tag{1}$$

- *Khe thời gian khám phá tuyến* là khoảng thời gian giữa hai lần khám phá tuyến được tính theo công thức 2, trong đó e_i là thời điểm nhận trả lời tuyến thứ i, s_{i+1} thời điểm thực hiện khám phá tuyến tiếp theo.

$$T = s_{i+1} - e_i \tag{2}$$

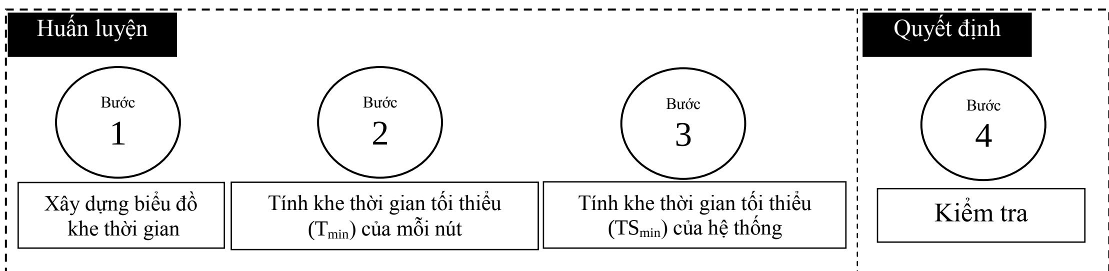
- *Khe thời gian khám phá tuyến tối thiểu của một nút* là khoảng thời gian tối thiểu giữa các lần khám phá tuyến tại một nút mạng được tính theo công thức 3, trong đó m là số lượng khe thời gian khám phá tuyến.

$$T_{\min} = Min(T_i); \forall i = \overline{1.m} \tag{3}$$

- *Khe thời gian khám phá tuyến tối thiểu của hệ thống* là khoảng thời gian tối thiểu giữa các lần khám phá tuyến trong toàn hệ thống được tính theo công thức 4, trong đó n là số lượng nút mạng.

$$TS_{\min} = Min(T_{\min}^{j}); \forall j = \overline{1.n} \tag{4}$$

Gói khám phá tuyến (RREQ) cho phép nút nguồn khám phá tuyến đến đích khi cần thiết, trong môi trường mạng bình thường thì số lần khám phá tuyến phụ thuộc vào nhu cầu định tuyến tại mỗi nút nên tầng suất khám phá tuyến thấp. Tuy nhiên, khi xuất hiện nút độc hại thực hiện hành vi tấn công ngập lụt gói RREQ thì tầng suất khám phá tuyến dày đặc, đây là đặc điểm mà chúng tôi sử dụng để xây dựng mô hình cho phép phát hiện nút độc hại như hình 2.



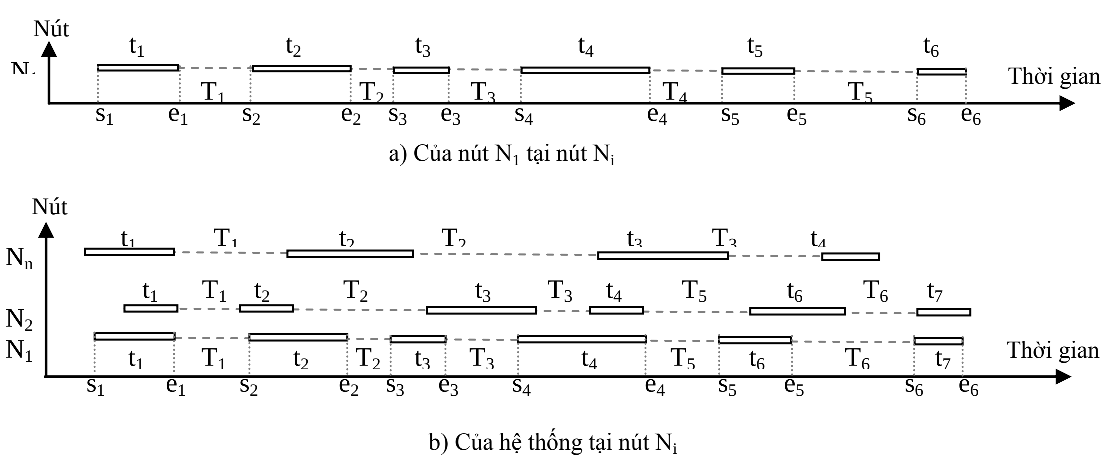
Hình 2. Mô hình kiểm tra an ninh của SMA nhằm phát hiện tấn công ngập lụt gói RREQ

Hình 2 cho thấy quá trình kiểm tra an ninh của SMA gồm hai giai đoạn cơ bản là *huấn luyện* và *kiểm tra*. Trong đó, giai đoạn kiểm tra chỉ được thực hiện sau khi thực hiện xong quá trình huấn luyện, chi tiết các bước như sau:

Bước 1: Trong giai đoạn huấn luyện, tất cả các nút sẽ thu thập thông tin khám phá tuyến của các nút khác trong hệ thống nhằm xây dựng biểu đồ khe thời gian, hình 3 mô tả biểu đồ khe thời gian tại nút N_i.

Bước 2: Sử dụng dữ liệu vào là biểu đồ khe thời gian khám phá tuyến được xây dựng tại bước 1, áp dụng công thức 3 để tính khe thời gian tối thiểu (T_{min}) của mỗi nút.

Bước 3: Dựa vào dữ liệu đã thu thập tại bước 1 và 2, áp dụng công thức 4 để tính khe thời gian tối thiểu (TS_{min}) của hệ thống. Đây là giá trị ngưỡng để kiểm tra an ninh tại bước 4.

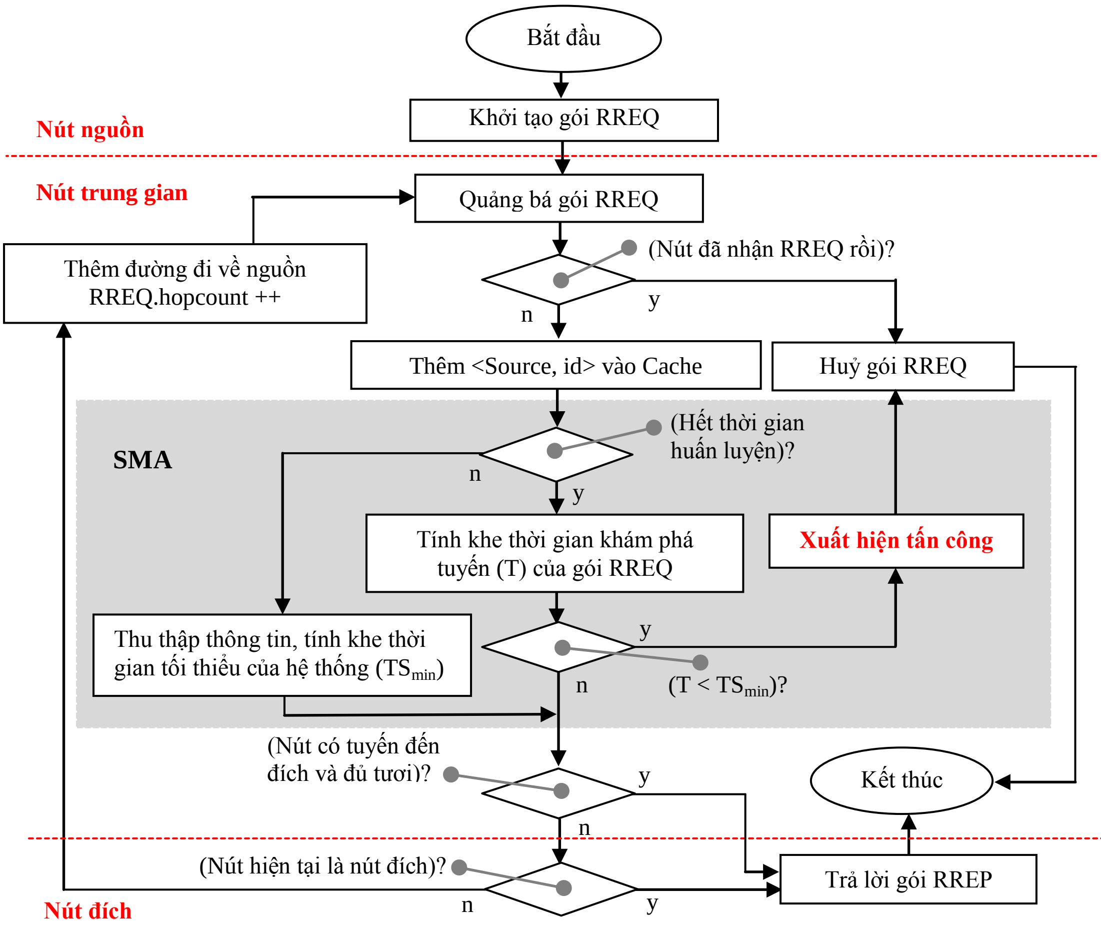


Hình 3. Biểu đồ khe thời gian khám phá tuyến

Bước 4: Khi hết thời gian huấn luyện, mỗi nút sẽ kiểm tra an ninh khi nhận được yêu cầu tuyến RREQ từ nút nguồn bất kỳ N_i. Nếu khe thời gian khám phá tuyến của nút N_i nhỏ hơn khe thời gian khám phá tuyến tối thiểu của hệ thống ($T < TS_{min}$) thì xuất hiện tấn công ngập lụt.

2. Đề xuất giao thức SMA-AODV

Giao thức AODV nguyên bản chấp nhận tất cả các gói RREQ khám phá tuyến từ nút nguồn bất kỳ, đây là điểm yếu bị tin tặc lợi dụng để thực hiện tấn công ngập lụt gói RREQ. Giải pháp của chúng tôi là tích hợp SMA vào quá trình khám phá tuyến của giao thức AODV tạo giao thức SMA-AODV có khả năng phát hiện tấn công ngập lụt gói RREQ, chi tiết thuật toán khám phá tuyến cải tiến được mô tả tại hình 4.



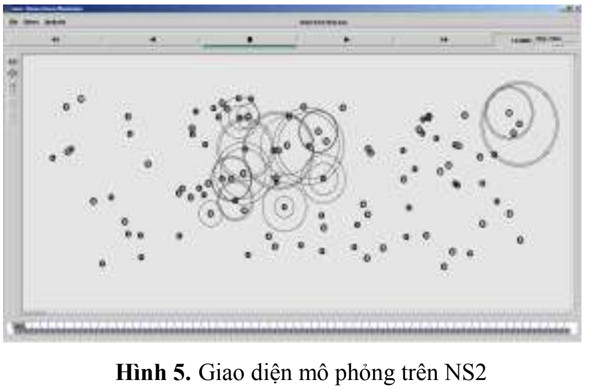
Hình 4. Thuật toán khám phá tuyến cải tiến trong giao thức SMA-AODV

Thuật toán khám phá tuyến trong SMA-AODV (hình 4) cho thấy trong giai đoạn huấn luyện thì giao thức SMA-AODV hoạt động như giao thức AODV, tất cả gói RREQ nhận được đều được chấp nhận và tiếp tục quảng bá gói RREQ đến tất cả láng giềng để khám phá tuyến. Điểm khác biệt so với AODV là tác tử SMA thu thập thông tin để tính khe thời gian tối thiểu của hệ thống (TS_{min}), đây là giá trị cơ sở để phát hiện tấn công ngập lụt gói RREQ, vì vậy yêu cầu trong giai đoạn này là hệ thống không được tồn tại nút độc hại. Sau giai đoạn huấn luyện, nút N_i kiểm tra an ninh gói RREQ nhận được từ N_j trước khi quảng bá đến láng giềng. Nếu khe thời gian khám phá tuyến (T) của gói RREQ nhỏ hơn khe thời gian khám phá tuyến tối thiểu của hệ thống (TS_{min}) thì xuất hiện tấn công ngập lụt, gói RREQ bị hủy.

IV. ĐÁNH GIÁ KẾT QUẢ BẰNG MÔ PHỎNG

1. Thông số mô phỏng và tiêu chí đánh giá

Chúng tôi sử dụng hệ mô phỏng NS2 [16] phiên bản 2.35 để đánh giá tác hại của các hình thức tấn công ngập lụt gói RREQ đến khả năng định tuyến của giao thức AODV và hiệu quả phát hiện tấn công của giao thức SMA-AODV. Tổng số 5 mô hình mạng được sử dụng để mô phỏng, mỗi mô hình mạng có 100 nút bình thường và 1 nút độc hại, hoạt động trong phạm vi 3200m x 1000m, các nút mạng chuyển động ngẫu nhiên với vận tốc di chuyển thay đổi tối đa 10m/s theo mô hình Random Waypoint [17], kịch bản được tạo bởi công cụ *./setdest* trên NS2.



Hình 5. Giao diện mô phỏng trên NS2

Bảng 1. Thông số mô phỏng trên NS2

Thông số	Giá trị
Khu vực địa lý	3200m x 1000m
Vùng thu phát sóng	250m
Thời gian mô phỏng	200s
Tổng số nút mạng	101 (1 nút độc hại)
Vận tốc di chuyển (m/s)	1..10
Dạng truyền thông	CBR (Constant Bit Rate)
Số kết nối	10 UDP
Kích thước gói tin	512(bytes)
Hàng đợi	FIFO (DropTail)
Giao thức định tuyến	AODV và MSA- AODV
Thời gian huấn luyện	49 giây

Giao thức mô phỏng là AODV và SMA-AODV, thời gian mô phỏng 200s, vùng phát sóng 250m, hàng đợi FIFO, có 10 kết nối UDP, nguồn phát CBR, kích thước gói tin 512 byte, nút độc hại đứng yên tại vị trí trung tâm (1600, 500) và thực hiện hành vi tấn công ngập lụt gói RREQ bắt đầu tại giây thứ 50, nguồn phát UDP đầu tiên bắt đầu tại giây thứ 0, các nguồn phát tiếp theo cách nhau 5 giây. Nút tham gia luồng dữ liệu (nút nguồn, đích) gồm {(0, 19); (3, 56); (6, 93); (21, 77); (41, 59); (62, 91); (65, 73); (80, 12); (84, 32); (99, 40)}. Trong quá trình mô phỏng có 5 nguồn phát CBR ngưng từ giây 100 đến giây 150 thì phát lại. Chi tiết các thông số mô phỏng được tổng hợp trong bảng 1.

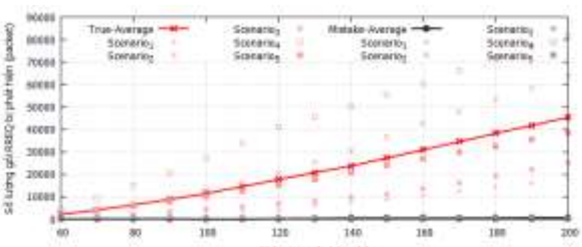
Để đánh giá tác hại của tấn công ngập lụt gói RREQ và giải pháp cải tiến giao thức AODV nhằm phát hiện tấn công, chúng tôi sử dụng một số tiêu chí là: Hiệu quả phát hiện gói RREQ độc hại, hiệu quả khám phá tuyến (gồm thời gian khám phá tuyến trung bình, số lần khám phá tuyến), tỷ lệ gửi gói tin thành công, thông lượng mạng, hao phí truyền thông, thời gian trễ trung bình.

- *Hiệu quả phát hiện gói RREQ độc hại:* Thông số cho biết khả năng phát hiện gói RREQ do nút độc hại sử dụng để thực hiện tấn công ngập lụt.
- *Hiệu quả khám phá tuyến:* Thông số cho biết tác hại của tấn công ngập lụt và hiệu quả an ninh của SMA-AODV, được đánh giá dựa vào *thời gian khám phá tuyến và số lần khám phá tuyến*.
- *Tỷ lệ gửi gói tin thành công:* Thông số cho biết tỷ lệ gói tin gửi đến đích/tổng số gói tin đã gửi.
- *Thông lượng mạng:* Là thông số đo lượng thông tin truyền thông, được tính bằng (tổng số gói tin gửi thành công * kích thước gói tin) / thời gian mô phỏng.
- *Hao phí truyền thông:* Thông số cho biết tổng số gói tin điều khiển tuyến đã gửi, hoặc chuyển tiếp tại tất cả nút mạng.
- *Thời gian trễ trung bình:* Thông số đo khoảng thời gian trung bình để định tuyến một gói dữ liệu thành công từ nguồn đến đích.

2. Kết quả mô phỏng

a) Hiệu quả phát hiện gói RREQ độc hại

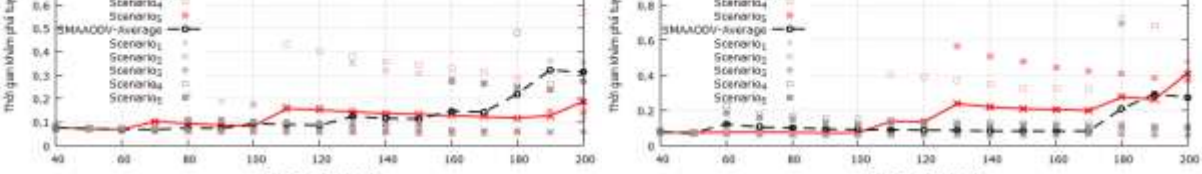
Biểu đồ số lượng gói RREQ độc hại bị phát hiện (hình 6) cho thấy sau 200s mô phỏng, giao thức SMA-AODV đã phát hiện 45285.8 gói RREQ độc hại trong tổng số 45814.8 gói RREQ bị phát hiện, tỷ lệ đúng là 98.85%. Số gói RREQ phát hiện sai lầm là 529 gói (tỷ lệ 1.15%), nguyên nhân là nút nguồn phát gói yêu cầu tuyến quá nhanh nên khe thời gian khám phá tuyến (T) nhỏ hơn khe thời gian khám phá tuyến tối thiểu của hệ thống (TS_{min}).



Hình 6. Số lượng gói RREQ độc hại bị phát hiện

b) Thời gian khám phá tuyến

Biểu đồ thời gian khám phá tuyến (hình 7) cho thấy sau 200 giây mô phỏng thì thời gian trung bình mỗi lần khám phá tuyến (ADRD) của AODV là 0.188s trong môi trường bình thường và 0.411s trong môi trường mạng bị tấn công, tăng **218.86%.** Giao thức SMA-AODV có khả năng phát hiện tấn công nên ADRD là 0.274s, chỉ bằng **66.64%** so với AODV khi bị tấn công. Như vậy, tấn công ngập lụt đã ngăn cản quá trình khám phá tuyến của giao thức AODV nên thời gian khám phá tuyến của AODV tăng cao khi bị tấn công, tuy nhiên khả năng an ninh đã làm giao thức SMA-AODV có ADRD cao hơn AODV trong môi trường bình thường.

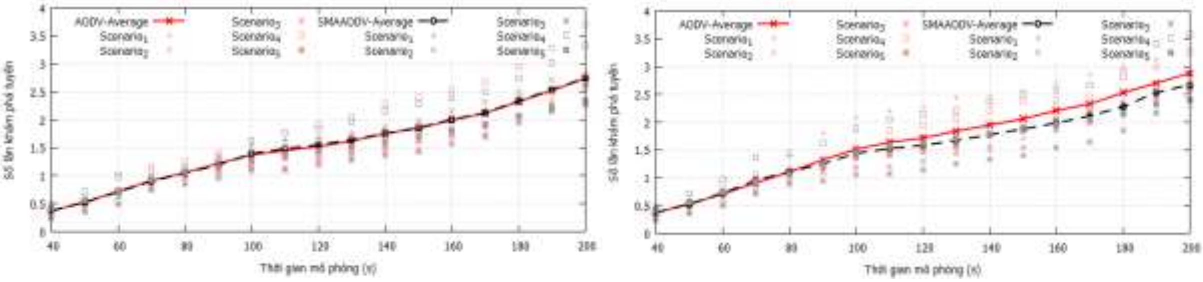


a) Bình thường *b) Tấn công Flooding RREQ*

Hình 7. Thời gian khám phá tuyến

c) Số lần khám phá tuyến

Biểu đồ số lần khám phá tuyến (hình 8) cho thấy sau 200s mô phỏng trong môi trường mạng bình thường thì trung bình số lần khám phá tuyến (ANDR) của hai giao thức gần tương đương nhau, AODV là 2.744 và SMA-AODV là 2.75. Tuy nhiên, trong môi trường mạng bị tấn công thì trung bình mỗi nút phải thực hiện 2.886 lần khám phá tuyến đối với AODV và 2.674 lần khám phá đối với SMA-AODV. Điều này cho thấy tấn công ngập lụt đã ngăn cản quá trình khám phá tuyến nên ANDR của giao thức AODV cao hơn SMA-AODV khi bị tấn công.

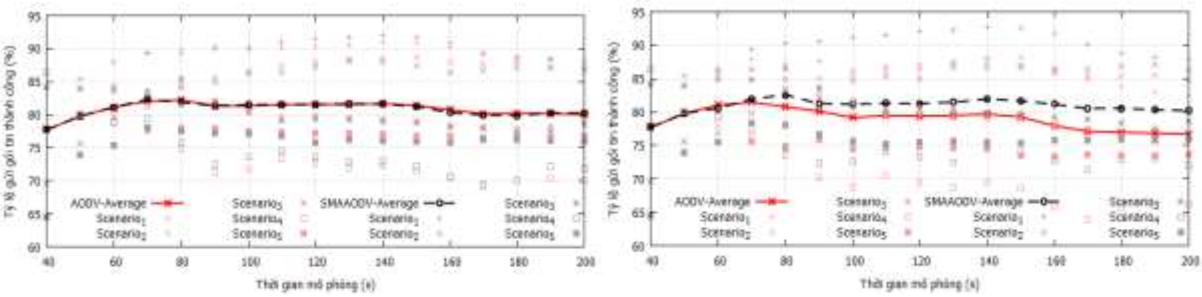


a) Bình thường *b) Tấn công Flooding RREQ*

Hình 8. Số lần khám phá tuyến tại mỗi nút

d) Tỷ lệ gửi gói tin thành công

Biểu đồ (hình 9) cho thấy tỷ lệ gửi gói tin thành công (PDR) của cả hai giao thức gần tương đương nhau trong môi trường mạng bình thường, AODV là 80.28% và SMA-AODV là 80.25%. Tuy nhiên, trong môi trường mạng bị tấn công thì PDR của AODV là 76.7% khi bị tấn công, giảm 3.58%. Điều này cho thấy tấn công ngập lụt đã ngăn cản quá trình khám phá tuyến nên đã làm giảm PDR của giao thức AODV. Ngược lại, giao thức SMA-AODV có thể phát hiện tấn công ngập lụt nên PDR của SMA-AODV khi bị tấn công chỉ thấp hơn 0.05% so với môi trường bình thường.

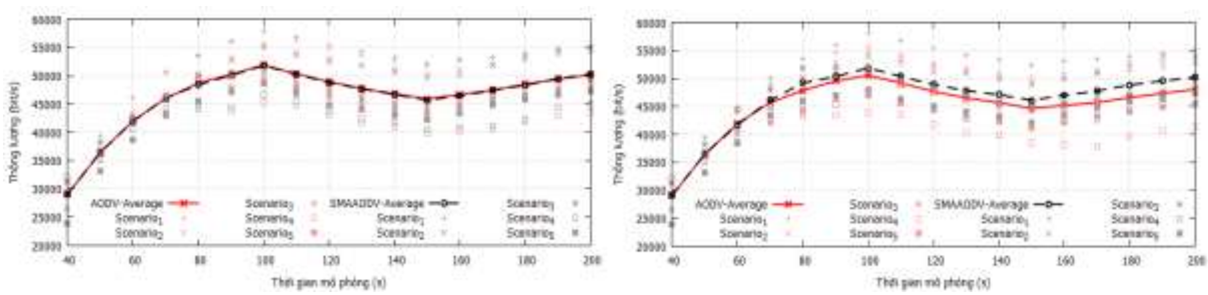


a) Bình thường *b) Tấn công Flooding RREQ*

Hình 9. Tỷ lệ gửi gói tin thành công

e) Thông lượng mạng

Biểu đồ (hình 10) cho thấy thông lượng mạng (TN) của cả hai giao thức gần tương đương nhau trong môi trường mạng bình thường, nguyên nhân là do PDR của chúng gần tương đương nhau. Tuy nhiên, trong môi trường mạng bị tấn công thì TN của giao thức AODV giảm nhiều, giao thức SMA-AODV có bị ảnh hưởng nhưng không đáng kể. Sau 200s mô phỏng, TN của AODV là 50315.27 bit/s trong môi trường mạng bình thường, giảm xuống 48058.4 bit/s khi bị tấn công. Ngược lại, SMA-AODV có thể phát hiện tấn công ngập lụt nên TN là 50290.70 bit/s trong môi trường mạng bình thường và 50237.44 bit/s khi bị tấn công.

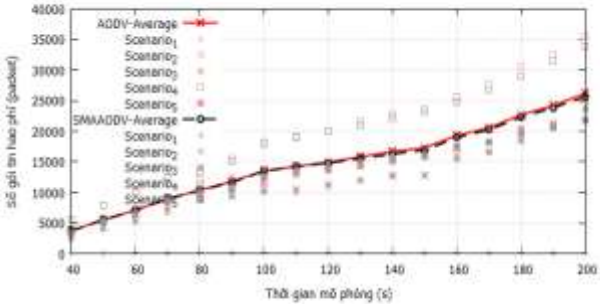


a) Bình thường *b) Tấn công Flooding RREQ*

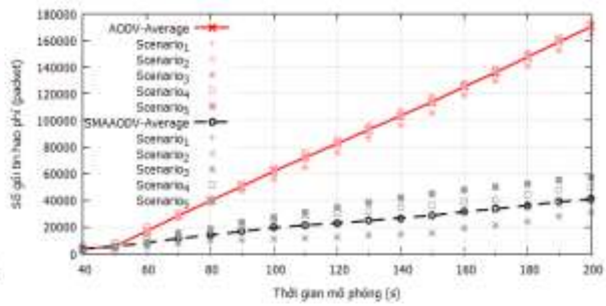
Hình 10. Thông lượng mạng

f) Hao phí truyền thông

Biểu đồ (hình 11) cho thấy hao phí truyền thông (CO) của cả hai giao thức gần tương đương nhau trong môi trường mạng bình thường. Tuy nhiên, hao phí truyền thông của AODV tăng **650.29%** khi bị tấn công, từ 26179.8 gói, tăng lên 170245 gói. Hao phí truyền thông của giao thức SMA-AODV cũng bị ảnh hưởng khi bị tấn công, tăng 160.28% từ 25623.6 gói tăng lên 41069.8 gói. Như vậy, giao thức SMA-AODV có thể phát hiện tấn công ngập lụt nên CO của SMA-AODV chỉ bằng **24.12%** so với AODV khi bị tấn công.



a) Bình thường

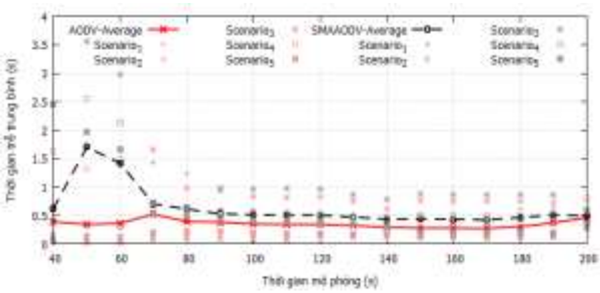


b) Tấn công Flooding RREQ

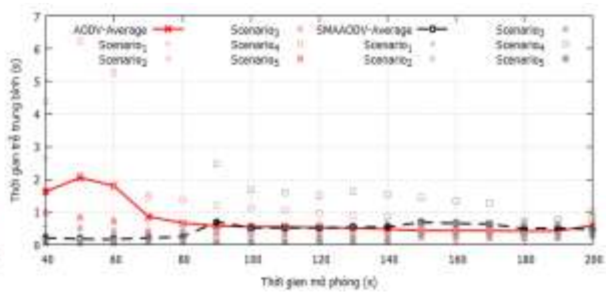
Hình 11. Hao phí truyền thông

g) Thời gian trễ trung bình (ETE)

Biểu đồ thời gian trễ trung bình (hình 12) cho thấy tấn công ngập lụt đã làm tăng thời gian định tuyến gói dữ liệu thành công đến đích của AODV. Sau 200 giây mô phỏng, ETE của AODV là 0.46s trong môi trường mạng bình thường và tăng lên 0.58s khi bị tấn công. ETE của SMA-AODV là 0.49s trong môi trường mạng bình thường và 0.46s khi bị tấn công.



a) Bình thường



b) Tấn công Flooding RREQ

Hình 12. Thời gian trễ trung bình

V. KẾT LUẬN

Như vậy, bài báo đã đề xuất tác tử di động an ninh (SMA) có khả năng phát hiện tấn công ngập lụt gói RREQ, và tích hợp vào AODV để tạo giao thức an ninh SMA-AODV. Kết quả mô phỏng cho thấy khi bị tấn công thì tỷ lệ gửi gói tin thành công (PDR) của SMA-AODV chỉ bị giảm **0.05%,** riêng AODV giảm **3.58%** và đặc biệt hao phí truyền thông của SMA-AODV giảm đáng kể, chỉ bằng 24.12% so với AODV. Riêng môi trường bình thường thì PDR của SMA-AODV chỉ thấp hơn **0.03%** so với AODV.

Tương lai, chúng tôi tiếp tục cải tiến SMA để cho phép phát hiện tấn công ngập lụt gói HELLO và DATA. Đồng thời, cài đặt đánh giá với các nghiên cứu đã công bố để kiểm chứng thêm kết quả.

VI. LỜI CẢM ƠN

Bài báo được thực hiện dưới sự hỗ trợ tài chính của đề tài khoa học công nghệ cấp Bộ Giáo dục và Đào tạo có mã số B2016-DHH-21.

TÀI LIỆU THAM KHẢO

[1] H. Jeroen, M. Ingrid, D. Bart, and D. Piet, "An overview of mobile ad hoc networks: Applications and challenges", Journal of the Communications Network, vol. 3, no. 3, pp. 60–66, 2004.

[2] E. Alotaibi and B. Mukherjee, "A survey on routing algorithms for wireless Ad-Hoc and mesh networks", Computer Networks, vol. 56, no. 2, pp. 940–965, 2012.

[3] T. Cholez, C. Henard, I. Chrisment, O. Festor, G. Doyen, and R. Khatoun, "A first approach to detect suspicious peers in the KAD P2P network", SAR-SSI Proceedings, pp. 1–8, 2011.

[4] Y. Ping, D. Zhoulin, Y. Zhong, and Z. Shiyong, "Resisting flooding attacks in ad hoc networks," ITCC'05, vol. 2, pp. 657 – 662, 2005.

[5] C. E. Perkins, M. Park, and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing", WMCSA, pp. 90–100, 1999.

[6] H. Ehsan and F. A. Khan, "Malicious AODV: Implementation and analysis of routing attacks in MANETs", IUCC-2012, pp. 1181–1187, 2012.

[7] F. C. Jiang, C. H. Lin, and H. W. Wu, "Lifetime elongation of ad hoc networks under flooding attack using power-saving technique", Ad Hoc Networks, vol. 21, pp. 84–96, 2014.

[8] M. G. Zapata, "Secure ad hoc on-demand distance vector routing", Mobile Computing and Communications Review, vol. 6, no. 3, pp. 106–107, 2002.

[9] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks", ICNP, pp. 78–89, 2002.

[10] Q. Li, M. Y. Zhao, J. Walker, Y. C. Hu, A. Perrig, and W. Trappe, "SEAR: a secure efficient ad hoc on demand routing protocol for wireless networks," Security and Communication networks, vol. 2, no. 4, pp. 325–340, 2009.

[11] M. Mohammadizadeh, A. Movaghar, and S. Safi, "SEAODV: Secure Efficient AODV Routing Protocol for MANETs Networks," ICIS 09, pp. 940–944, 2009.

[12] P. Yi, Y. Hou, Y. Bong, S. Zhang, and Z. Dui, "Flooding Attacks and defence in Ad hoc networks," Journal of Systems Engineering and Electronics, vol. 17, no. 2, pp. 410– 416, 2006.

[13] S. Desilva and R. V. Boppana, "Mitigating malicious control packet floods in ad hoc networks," IEEE Wireless Communications and Networking Conference (WCNC), vol. 4, pp. 2112–2117, 2005

[14] V. Balakrishnan, V. Varadharajan, and I. Group, "Mitigating Flooding Attacks in Mobile Ad-hoc Networks Supporting Anonymous Communications", AUSWIRELESS '07 Proceedings, pp. 29-34, 2007.

[15] R. P. Ankala, D. Kavitha, and D. Haritha, "Mobile agent based routing in MANETS – attacks & defences", Network Protocols and Algorithms, vol. 3, no. 4, pp. 108–121, 2011.

[16] The network simulator NS2, URL:http://www.isi.edu/nsnam/ns/

[17] J. Yoon, M. Liu, and B. Noble, "Random waypoint considered harmful", IEEE Infocom 2003, vol. 2, pp. 1–11, 2003.

[18] H. L. Nguyen and U. T. Nguyen, "A study of different types of attacks on multicast in mobile ad hoc networks", Ad Hoc Networks, vol. 6, no. 1, pp. 32–46, 2008.

A SOLUTION TO DETECT FLOODING ATTACKS IN MANET

Luong Thai Ngoc, Vo Thanh Tu

ABSTRACT*—The flooding attacks prevent discovery route process and increase communication overhead of AODV routing protocol in Mobile Ad hoc Network. In this article, we describe a solution to build security mobile agent (SMA), and integrating SMA into the discovery route process of AODV procotol. Improved protocol is called SMA-AODV which can detect flooding attacks. Using NS2, we compare the performance of SMA-AODV and AODV with mobility nodes network topology under flooding attacks.*